U.S. Department of Justice

United States Attorney
Western District of Washington

Please reply to:
S. Kate Vaughan
Assistant United States Attorney
Direct Line: (206) 553-4148

700 Stewart Street, Suite 5220
Seattle WA, 98101-1271
www.usdoj.gov/usao/waw

Tel: (206) 553-7970
Fax: (206) 553-0882

October 30, 2015

Linda Sullivan,
Colin Feiman,
Assistant Federal Public Defenders,
Office of the Federal Public Defender,
Tacoma, WA

Re: *United States v. Jay Michaud*
No. CR15-5351 RJB, USDC, W.D. Washington

Dear Ms. Sullivan, Mr. Feiman:

We write in response to your discovery requests dated September 9, September 23, and October 22, 2015. As you are aware, Federal Rule of Criminal Procedure 16(D), "Documents and Objects," provides that:

> [upon a defendant's request], the government must permit the defendant to inspect and to copy or photograph books, papers, documents, data, photographs, tangible objects, buildings or places, or copies or portions of any of these items, if the item is within the government's possession, custody, or control and: (i) the item is material to preparing the defense; (ii) the government intends to use the item in its case-in-chief at trial; or (iii) the item was obtained from or belongs to the defendant.

With respect to your requests for information about the court-authorized Network Investigative Technique ("NIT"), including the name of the agency or company that developed the program, a copy of the NIT programming code, a detailed description of the computer instructions that are downloaded onto target computers, and a detailed description of the means by which these instructions are introduced to target computers: that information does not consist of evidence the government intends to use in its case-in-chief at trial, it was not obtained nor does it belong to your client, and the government does not believe (nor have you indicated why) that information is material to your client's defense. Moreover, the detailed information about the investigative technique requested, including the programming code, is subject to law enforcement privilege, which the government hereby asserts.

The information that was collected through use of the court-authorized NIT, however, has been made available for your review and will remain so during the pendency of this litigation, pursuant to the current protective order. Specifically, that information is contained in the user report that was made available to you for review on October 29, 2015. A copy of that user report, redacted of digital images (that include illegal child pornography), was also provided to you on October 29, 2015.

Without waiving any argument regarding the materiality or the privileged nature of the information requested, we provide the following responses to your specific questions.

In response to your September 9, 2015, letter:

- **The actual name of the NIT software or program**

There is no particular name for the NIT code.

- **The name of the agency or company that developed the program**

The information requested is not material to your client's defense and subject to law enforcement privilege. Accordingly, the government declines to provide that information.

- **A detailed description of the "additional computer instructions" that are downloaded onto target computers and a copy of the NIT's programming code**

The computer instructions downloaded onto a target's computer (hereinafter "activating" computer) directed the "activating" computer to transmit the following information to a computer controlled by or known to the government:

1. The "activating" computer's actual IP address, and the date and time that the NIT determined what the IP address is;
2. A unique identifier generated by the NIT (e.g. a series of numbers, letters, and/or special characters) to distinguish the data from that of other "activating" computers. That unique identifier was sent with and collected by the NIT;
3. The type of operating system running on the computer, including type (e.g., Windows), version (e.g. Windows 7), and architecture (e.g., x 86);

4. Information about whether the NIT had already been delivered to the "activating" computer;
5. The "activating" computer's "Host Name." A Host Name is a name assigned to a device connected to a computer network that is used to identify the device in various forms of electronic communication, such as communications over the Internet;
6. The "activating" computer's active operating system username; and
7. The "activating" computer's Media Access Control ("MAC") address. The equipment that connects a computer to a network is commonly referred to as a network adapter. Most network adapters have a MAC address assigned by the manufacturer of the adapter that is designed to be a unique identifying number. A unique MAC address allows for proper routing of communications ton a network. Because the MAC address does not change and is intended to be unique, a MAC address can allow law enforcement to identify whether communications sent or received at different times are associated with the same adapter.

- **A detailed description of the means by which these instructions are introduced to target computers**

In the normal course of operation, websites send content to a visitor's computer. In accordance with the search warrant authorizing the use of the NIT, when an "activating" computer requested content from Website A, Website A augmented the requested content with the additional computer instructions associated with the NIT.

- **Complete copy of all information and data that was received by the Government in connection with Mr. Michaud's case by means of the NIT**

This information is contained in the user report that was made available for your review on October 29, 2015, and was also provided to you on a CD on the same date (redacted of digital images that include illegal child pornography).

As reflected in the data that has been made available for your review in the user report, the following actions can be attributed to Mr. Michaud. On February 28, 2015, after logging on to the website with the previously established username "Pewter," Mr. Michaud, using his Windows computer with hostname "Main" and Windows Username "Gullible," navigated to the section of the website entitled "Pre-teen Videos >> Girls HC." In the context of the website, HC was an abbreviation for "hardcore." After

accessing this section of the website, Mr. Michaud clicked on a specific post entitled, "Girl 12ish eats other girls/dirty talk." This particular post purported to contain links to images and videos of child pornography. The NIT was deployed to Mr. Michaud's computer after he opened this particular post in the "Pre-teen Videos >> Girls HC" section.

Using the Pewter account, Mr. Michaud also accessed approximately 187 different posts on the website between February 20, 2015 and March 4, 2015. The titles and content of those posts, which are mostly indicative of containing hardcore child pornography, can be viewed in the user report.

Please note that only a limited set of information was collected through the court-authorized use of the NIT, which information is specified above and in the user report. Other information about user activity, such as the pages and postings accessed, was collected through request data and website logs which were not a function of the NIT.

- **Copies of the target site's web pages as they appeared at the time(s) Mr. Michaud allegedly accessed the site**

An offline copy of the website, as it appeared to users, is being made available for your review and inspection at the FBI office in Seattle on Wednesday November 4, 2015. We will continue to make that offline copy available for your review and inspection during the pendency of this litigation. Please feel free to make arrangements to re-review the site on further occasions as necessary.

On October 29, 2015, we made image copies of your client's digital media available for review at the FBI facility in Tacoma. We will continue to make those images available for your review and inspection, at the FBI facility in Vancouver, Washington, where you and your designated forensic examiner will be allowed to conduct appropriate analysis on that data and to consult in private about that analysis. Please let Special Agent Mautz know when you would like to make arrangements for review of those image copies, he can be reached at (360) 695 5661. Please let us know if you have questions about that arrangement.

You also requested that we "identify any federal warrant applications that have sought permission to use the NIT or similar software or programs and were denied by the judge, in any district, to whom an application was presented." As you are aware, the

deployment of the NIT utilized in this case was authorized by the United States District Court for the Eastern District of Virginia. No court denied an application to deploy the NIT used in this case. To the extent that you request information about other, different investigative techniques than the one used in this case, we do not believe that information to be material to this case.

In response to your September 23, 2015, letter:

- **copies of the target site's web pages as they appeared at the time(s) Mr. Michaud allegedly accessed the site:**

Please see the above response regarding the offline copy of the website, which will remain available for your review and inspection.

- **copies of any court authorizations for control and operation of the target site by law enforcement.**

No court authorization is required in order for a law enforcement agency to control and operate a website under U.S. law. In any event, you have been provided with the search warrant authorizing the deployment of a NIT on Website A and a Title III authorization permitting the monitoring of electronic communications of site users, along with accompanying paperwork.

In response to your October 22, 2015, letter:

You made a number of requests for information about pictures, videos and links that were posted, viewed or downloaded by visitors other than your client, as well as for the number of visitors, visits, and length of visits between February 20 and March 4, 2015. As noted above, you have been given access to reports and information documenting the actions that your client took on the website between February 20 and March 4, 2015. The government does not believe that the actions of users other than your client are material to your client's defense in this case. Nonetheless, to the extent that you are interested in the actions of users other than your client on the website, you and your investigators are welcome to review the offline copy of the website in order to determine the requested information. We will continue to make that available for your inspection and review so that you may do so.

You also requested:
A summary of any measures that were taken by the FBI or other law enforcement entities to block access to the pictures, videos and links available on or through the site between February 20 and March 4, 2015; the reason the site was shut down on March 4 (rather than earlier or later); and all documents relating to review and authorization of the FBI's administrative control of the site by the Department of Justice or other governmental agencies that were involved in the "Website A" investigation and deployment of the NIT at issue in our case.

As you are aware, Fed. R. Crim. P. 16(a)(2) "does not authorize the discovery or inspection of reports, memoranda, or other internal government documents made by an attorney for the government or other government agent in connection with investigating or prosecuting the case." The requested information is subject to law enforcement privilege, which the government hereby asserts, and/or other privileges pertaining to the deliberations of government attorneys or officials. Moreover, based upon the information provided in your request, the requested information does not appear to be material your client's defense. Accordingly, the requested information is neither material nor discoverable and the government declines to provide answers to those requests.

Please feel free to contact us with any further questions.

Sincerely,

ANNETTE L. HAYES
United States Attorney

/s/ S. Kate Vaughan
S. KATE VAUGHAN
Assistant United States Attorney

/s/ Keith Becker
KEITH BECKER
Assistant United States Attorney